Data Protection Policy	
Policy ref:	**ORG-10**
Approved:	February 2019
Due for Review:	2020
To be read in conjunction with:	ORG-09 Privacy Policy

Data Protection Policy

1. Introduction

This Policy sets out the way in which Cumbria Wildlife Trust (the Trust) will process personal data from the point of collection, throughout its use and for the duration of its storage, whether it is in paper or electronic form. Through the application of this Policy the Trust will meet its legal requirements under the Data Protection Act 2018 (DPA), the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications Regulations (PECR) and other applicable legislation.

The Policy applies:

- to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system;
- to all Trust staff, including volunteers, and all those who process data on the Trust's behalf.

The Trust's Finance and Administration Manager and all those in managerial or supervisory roles throughout the Trust are responsible for developing and encouraging good information handling practices within the Trust.

2. Definitions

Personal data – any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category data – personal data that the GDPR defines as more sensitive such as information about an individual's race, ethnic origin, politics, religious or philosophical beliefs, trade-union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

Criminal offence data – personal data relating to criminal convictions and offences, or related security measures.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The Trust is a data controller under GDPR.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. For the purposes of this policy, a child will be as defined by the DPA, that is, anyone of less than 13 years old.

Data protection impact assessment (DPIA) - a process which helps to identify and minimise the data protection risks of a project. A DPIA is required for processing that is likely to result in a high risk to individuals. This includes some specified types of processing. It is good practice to also do a DPIA for any other major project which requires the processing of personal data.

Data protection officer (DPO) – DPOs assist a data controller to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. Under the terms of the GDPR, the Trust is not obligated to have a DPO. The Trust's Finance and Administration Manager (FAM) will be the Trust's main reference point for data protection matters.

Data register – a document that records data processing activities including the nature, purpose and retention period of all data held.

Data subject – any living individual who is the subject of personal data held by an organisation.

Data subject consent - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Direct marketing - the communication (by whatever means) of advertising or marketing material which is directed to particular individuals.

EEA - European Economic Area.

Filing system – any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Privacy information – information which must be provided to individuals about the collection and use of their personal data including the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. This need not be provided if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour.

Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or

otherwise processed. Where a breach is likely to have a material adverse effect on the personal data or privacy of the data subject there is an obligation on the data controller to report that breach to the supervisory authority which, in the UK, is the Information Commissioner's Office (ICO).

Subject access request procedure – the process outlined in this Policy, in particular see 7.2, for responding to a data subject's request for a copy of the data that the Trust holds in relation to them.

Third party – a natural or legal person, public authority, agency or body **other** than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

3. Summary

In accordance with the six data protection principles set out in section 6 below, the Trust will:

- Process personal data lawfully, fairly and in a transparent manner.
- Collect personal data only for specified, explicit and legitimate purposes.
- Process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Keep accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Keep personal data only for the period necessary for processing.
- Adopt appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing and accidental loss, destruction or damage.

The Trust will tell individuals (in its privacy notices) the reasons for processing their personal data, how it uses such data and the legal basis for processing. It will not process personal data of individuals for other reasons.

4. Policy statement

4.1. The Trust is committed to compliance with the GDPR and all other relevant laws in respect of personal data and the protection of the "rights and freedoms" of individuals whose information the Trust collects and processes.

4.2. Compliance with those laws is described by this policy and its connected processes and procedures.

4.3. The GDPR and this policy apply to all of the Trust's personal data processing functions including those performed on the personal data of customers, clients, employees, suppliers and partners and any other personal data the Trust processes from any source.

4.4. The Trust's FAM is responsible for reviewing the register of processing annually in the light of any changes to the Trust's activities (as determined by changes to the Data Register) and to any additional requirements identified by means of Data Protection Impact Assessments. This register needs to be available at the supervisory authority's request.

4.5. This policy applies to employees, staff, consultants and volunteers of the Trust including any outsourced suppliers. Any breach of the GDPR will be dealt with under the Trust's disciplinary policy and may also be a criminal offence in which case the matter will be reported as soon as possible to the appropriate authorities.

4.6. Partners and any third parties working with or for the Trust, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the Trust without having first entered into a data confidentiality agreement which imposes on the third party obligations no less onerous than those to which the Trust is committed and which gives the Trust the right to audit compliance with the agreement.

5. Responsibilities and roles under the General Data Protection Regulation

5.1. The Trust's FAM has specific responsibilities in respect of procedures such as the subject access request procedure and is the first point of call for staff seeking clarification on any aspect of data protection compliance.

5.2. Compliance with data protection legislation is the responsibility of all staff of the Trust who process personal data.

5.3. All of the Trust's staff will receive data protection compliance training appropriate to their roles.

5.4. The Trust's employees are responsible for ensuring that any personal data about them and supplied by them to the Trust is accurate and up-to-date.

6. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. The Trust's policies and procedures are designed to ensure compliance with those principles.

6.1. Personal data must be processed lawfully, fairly and transparently
Lawfully: a lawful basis must be identified before personal data can be processed. These are set out in section 8 of this Policy.

Fairly: personal data should only be processed in ways that people would reasonably expect and should not be used in ways that have unjustified adverse effects on them. Whether or not data is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived or misled when the personal data is obtained, processing it is unlikely to be fair.

Transparently: the GDPR includes rules on giving privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

As a minimum, the following information will be provided by the Trust to the data subject unless the individual already has the information or it would involve a disproportionate effort to provide it to them:

6.1.1. the identity and the contact details of the data controller;
6.1.2. as the Trust is not required to have a DPO, the contact details of the Trust's FAM;
6.1.3. the purposes of the processing for which the personal data is intended as well as the lawful basis for the processing;

6.1.4. the period for which the personal data will be stored;
6.1.5. the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
6.1.6. the categories of personal data concerned;
6.1.7. where applicable, the recipients or categories of recipients of the personal data including anyone who will process the data on the Trust's behalf;
6.1.8. where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
6.1.9. any further information necessary to guarantee fair processing.

6.2. Personal data can only be collected for specific, explicit and legitimate purposes
Data obtained for specified purposes must not be used for a purpose that differs from those formally recorded as part of the Trust's register of processing.

6.3. Personal data must be adequate, relevant and limited to what is necessary for processing
6.3.1. The FAM is responsible for ensuring that the Trust does not collect information that is not strictly necessary for the purpose for which it is obtained.
6.3.2. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to the privacy statement and be approved by the FAM.
6.3.3. The FAM will ensure that all data collection methods are reviewed annually to ensure that collected data continues to be adequate, relevant and not excessive.

6.4. Personal data must be accurate and kept up to date with every reasonable effort made to erase or rectify inaccurate data without delay
6.4.1. Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
6.4.2. The FAM is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
6.4.3. It is also the responsibility of the data subject to ensure that data held by the Trust is accurate and up to date.
6.4.4. Employees, volunteers and consultants are required to notify the Trust of any changes in circumstances to enable personal records to be updated accordingly. It is the responsibility of the Trust to ensure that any notification regarding a change of circumstances is recorded and acted upon.
6.4.5. The FAM is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
6.4.6. On at least an annual basis, the FAM will review the retention dates of all the personal data processed by the Trust, by reference to the Data Register, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure.
6.4.7. The FAM is responsible for responding to requests for rectification from data subjects within one month (see 7.3 below).
6.4.8. The FAM is responsible for making appropriate arrangements to ensure that where third-party organisations may have been passed inaccurate or out-of-date personal data they are informed of that fact and instructed not to use that data to inform decisions about the individuals concerned. The FAM will ensure that data corrections are passed to the third party if required.

6.5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing

6.5.1. Personal data will be retained in line with the Data Register and, once its retention date is passed, it must be securely destroyed as set out in section 11 of this Policy.

6.5.2. The FAM must specifically approve any data retention that exceeds the retention periods defined in the Data Register, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be in writing.

6.6. Personal data must be processed in a manner that ensures appropriate security
The FAM will carry out a risk assessment taking into account all the circumstances of the Trust's controlling or processing operations and the technical and organisational security measures that are in place.

In determining appropriateness, the FAM should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on the Trust itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the FAM will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy-enhancing technologies such as pseudonymisation and anonymisation;
- International security standards relevant to the Trust.

When assessing appropriate organisational measures the FAM will consider the following:

- Relevant training provision throughout the Trust;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Physical access controls to electronic and paper-based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on organisations receiving data from the Trust to take appropriate security measures when data is to be transferred outside the EEA.

These controls have been selected on the basis of identified risks to personal data and the potential for damage or distress to individuals whose data is being processed.

6.7. The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The Trust will, through appropriate management, training and the implementation and review of policies and procedures, ensure that all staff and volunteers are aware of this policy and their responsibilities under the Act.

The Trust will ensure that:

- everyone processing personal data on its behalf understands that they are responsible for adhering to this policy;
- data protection training is provided to all staff;
- the principles of data protection are integrated into all of the Trust's data processing activities from the outset (that is, "data protection by design");
- the Trust's approach to processing personal data is documented, regularly assessed and evaluated for compliance with the Act.

7. Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

7.1. The right to be informed
Individuals have the right to be informed about the collection and use of their personal data. At the time data is collected, the Trust will provide 'privacy information' including the purposes for processing their personal data, retention periods for that personal data and who data will be shared with.

7.2. The right of access (commonly referred to as 'subject access')
Individuals have the right to obtain a copy of their personal data as well as other supplementary information. The FAM will log subject access requests at the earliest opportunity and ensure that the Trust responds within one month in accordance with the requirements of the GDPR and DPA.

7.3. The right to rectification
Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. The FAM will log requests for rectification at the earliest opportunity and ensure that the Trust responds within one month in accordance with the requirements of the GDPR and DPA. If the Trust decides not to comply with the request, the FAM must respond to the data subject to explain the Trust's reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

7.4. The right to erasure (also known as 'the right to be forgotten')
Individuals have the right to have personal data erased, but only in certain circumstances. The Trust will respond to such requests within one month to confirm that the data has been erased or to confirm the circumstances under which it has been erased only partially or not at all and to inform the data subject of their right to complain to the ICO.

7.5. The right to restrict processing
Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. The Trust will respond to such requests as soon as practicable and in any event within one month.

7.6. The right to data portability

Individuals have the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller. This right only applies when the lawful basis for processing this information is consent or for the performance of a contract and the processing is being carried out by automated means. Where practicable, the Trust will supply the requested data within one month.

7.7. The right to object to processing
In certain circumstances individuals have the right to object to processing of their data. The applicable circumstances depend on the purposes and lawful basis of the processing. They have an absolute right to object to the processing of personal data if it is for direct marketing purposes. The Trust will respond to such requests as soon as practicable and in any event within one month.

7.8. The right to object to automated decision-making or to profiling
Individuals have the right to object to any automated profiling that is occurring without consent. The Trust will, as soon as practicable and in any event within one month, cease such profiling unless it is necessary for the performance of a contract with the individual or is authorised by law. The Trust will also adhere to the other requirements of the GDPR concerning such processing.

It should be noted that where a request under the above rights is manifestly unfounded or excessive a data controller can charge a reasonable fee or refuse to deal with the request.

8. Lawful basis for processing personal data

The Trust will only process personal data where it has a lawful basis for doing so and that basis has been documented and published in the Trust's Privacy Policy prior to the commencement of processing.

The GDPR sets out six lawful bases, two of which are not relevant to the Trust. The lawful bases on which the Trust will rely are:

8.1. Consent: the individual has given clear consent for the Trust to process their personal data for a specific purpose.
- 8.1.1. The Trust understands 'consent' to mean that it has been explicitly and freely given, and is a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them. The data subject can withdraw their consent at any time.
- 8.1.2. When seeking to obtain consent, the Trust will ensure that the data subject has been fully informed of the intended processing and has signified their agreement while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.
- 8.1.3. The Trust will not infer consent from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.
- 8.1.4. For sensitive data, explicit written consent of data subjects will be obtained unless an alternative legitimate basis for processing exists.
- 8.1.5. Where the Trust provides online services to children under the age of 13, parental or custodial authorisation must be obtained.

8.2. Contract: the processing is necessary for the Trust to perform a contract with the individual, or because they have asked the Trust to take specific steps (e.g. providing a quotation) before entering into a contract.

8.2.1. 'Necessary' does not mean that the processing must be essential for the purposes of performing a contract or taking relevant pre-contractual steps. However, the processing must be necessary for the Trust to deliver its side of the contract with this particular person; it must be a targeted and proportionate way of achieving that purpose.

8.2.2. The contract need not be in writing as long as there is an agreement which meets the requirements of contract law.

8.2.3. This lawful basis does not apply if there are other reasonable and less intrusive ways to meet for the Trust to meet its contractual obligations or take the steps requested.

8.3. Legal obligation: the processing is necessary for the Trust to comply with a legal obligation to which it is subject (not including contractual obligations).

8.3.1. This does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. It therefore includes clear common law obligations.

8.3.2. It does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that the overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

8.3.3. The processing need not be essential in order to comply with the legal obligation but it must be a reasonable and proportionate way of achieving compliance. This lawful basis cannot be relied upon if the Trust has discretion over whether to process the personal data or if there is another reasonable way to comply.

8.3.4. Where processing is on the basis of legal obligation, the individual has no right to erasure, right to data portability or right to object.

8.3.5. If asked to justify the processing, the Trust must be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly, for example, a government website or industry guidance that explains generally applicable legal obligations.

8.4. Legitimate interests: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

8.4.1. When processing personal data on the basis of its legitimate interests, the Trust will:

- identify the particular legitimate interest that is applicable
- be able to demonstrate that the processing is necessary for that purpose
- check that the individual's interests do not override the legitimate interest.

8.4.2. A wide range of interests may be legitimate interests. They can be the Trust's own interests or the interests of third parties, and commercial interests as well as wider societal benefits. For example, the Trust can rely on legitimate interests for marketing activities if it can show that the way the data is used is proportionate, has a minimal privacy impact and people would not be surprised or likely to object (but only if consent is not required under PECR). Legitimate interests may be

compelling or trivial, but trivial interests may be more easily overridden by the interests of the individual.

8.4.3. 'Necessary' means that the processing must be a targeted and proportionate way of achieving the purpose. Legitimate interests cannot be relied upon if there is another reasonable and less intrusive way to achieve the same result.

8.4.4. If the data subject would not reasonably expect the Trust to use data in that way, or it would cause them unwarranted harm, their interests are likely to override those of the Trust. However, the Trust's interests do not always have to align with the individual's interests. If there is a conflict, the Trust's interests can still prevail as long as there is a clear justification for the impact on the individual.

9. Processing special category data

Prior to processing special category data, the Trust will ensure that the processing satisfies one or more of the special category conditions of Article 9(2) of the GDPR and the additional conditions and safeguards of Schedule 1 of the DPA.

10. Processing criminal offence data

Prior to processing criminal offence data, the Trust will ensure that the processing complies with Article 10 of the GDPR and the additional conditions and safeguards of Schedule 1 of the DPA.

11. Security of data

11.1. All staff are responsible for ensuring that any personal data that the Trust holds and for which they are responsible is kept securely and is not in any circumstance disclosed to any third party unless that third party has been specifically authorised by the Trust to receive that information and has entered into a confidentiality agreement.

11.2. All personal data should be accessible only to those who need to use it and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with the Cyber Security Policy and/or
- stored on (removable) computer media which are encrypted in line with that policy

11.3. Care must be taken to ensure that computer screens and other display equipment are not visible except to authorised employees, contractors, secondees or volunteers of the Trust. All employees, contractors, secondees or volunteers are required to enter into a confidentiality agreement before they are given access to organisational information of any sort.

11.4. Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation from the FAM. As soon as manual records are no longer required for day-to-day client support, they must be removed for secure archiving in line with the Data Register.

11.5. Personal data may only be deleted or disposed of in line with the Data Register. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

11.6. Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised by the FAM to process data off-site.

12. Disclosure of data

12.1. The Trust must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies and, in certain circumstances, the Police. All employees, contractors, secondees or volunteers should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Trust's business.

12.2. The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safe guard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the FAM.

13. Retention and disposal of data

13.1. The Trust will not keep personal data in a form that permits identification of data subjects for a longer period than is necessary in relation to the purpose(s) for which the data was collected.

13.2. The Trust may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

13.3. The retention period for each category of personal data will be set out in the Data Register along with the criteria used to determine this period including any statutory obligations the Trust has to retain the data.

13.4. The Trust's data retention and data disposal procedures will apply in all cases.

13.5. Personal data must be disposed of in a secure manner, thereby protecting the "rights and freedoms" of data subjects.

14. Data transfers

14.1. Transfers of personal data within the EEA will be made in a way that prevents access by anyone other than the intended recipient(s).

14.2. All exports of data from within the EEA to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects". If personal data is to be transferred outside of the EEA, the Trust will ensure that it complies with the relevant legislation.

15. Risks to data

15.1. The Trust is aware of risks associated with the processing of particular types of personal data.

15.2. The Trust assesses the level of risk to individuals associated with the processing of their personal data. DPIAs are carried out by the Trust in relation to processing which is likely to result in a high risk to individuals' personal data including where that processing is undertaken by other organisations on the Trust's behalf.

15.3. The Trust will manage any risks identified by the impact assessment in order to reduce the likelihood of a non-conformance with this policy.

15.4. Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Trust shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

15.5. Where, as a result of a DPIA, it is clear that the Trust is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not the Trust may proceed must be escalated for review to the FAM.

15.6. The FAM shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

15.7. Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the Trust's risk management register and the requirements of the GDPR.

16. Electronic communications

16.1. The Trust will not carry out direct marketing to individuals by electronic means (including email, fax, automated telephone calls, automated text or other electronic message) without their consent.

16.2. All direct marketing carried out electronically with the individual's consent will be conducted in accordance with the PECR and any other relevant legislation.

16.3. The Trust will maintain clear records to show what each individual has consented to, when this consent was given and how the consent was communicated to the Trust.